PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-303440
(43)Date of publication of application : 28.10.1994

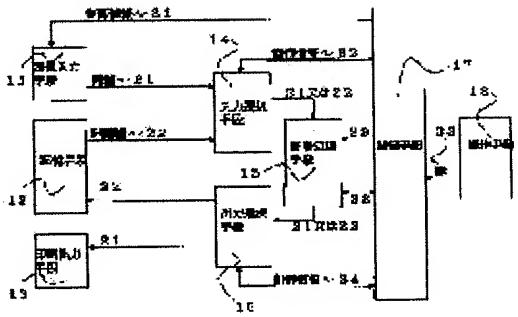
(51)Int.Cl. H04N 1/44
G03G 21/00
G09C 5/00
H04N 1/00

(21)Application number : 05-121824
(22)Date of filing : 14.04.1993

(71)Applicant : PANPUKIN HOUSE:KK
(72)Inventor : SASAKI MINORU
YOSHIKAWA HIROHARU

(54) COPYING MACHINE WITH CRYPTOGRAPHIC FUNCTION

(57)Abstract:
PURPOSE: To protect contents against an illegal read by storing a storage means or portable storage means with image information on a document or drawing to be stored in a ciphered state.
CONSTITUTION: The document or drawing is inputted as the image information 21 by selecting an image input means 11 by an input image selecting means 14, and then sent to a ciphering process means 15, which ciphers the information by using a set cipher key 23. The ciphered image information 22 after being sent to an output selecting means 16 is outputted to and stored in the storage means 12. Then when the information is deciphered, the ciphered image information 22 is inputted as input data from the input selecting means 14 and sent to the ciphering process means 15, which deciphers the information by using the cipher key 23. The deciphered image information 21 is sent by an output selecting means 16 to a printing output means 13 to print out the image information on the original document or drawing on a form.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision

of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平6－303440

(43)公開日　平成６年(1994)10月28日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｎ　1/44		7232－5C		
Ｇ０３Ｇ　21/00				
Ｇ０９Ｃ　5/00		8837－5L		
Ｈ０４Ｎ　1/00	Ｅ	7232－5C		

審査請求　未請求　請求項の数９　書面　（全 10 頁）

(21)出願番号　特願平5－121824

(22)出願日　平成５年(1993)４月14日

(71)出願人　393009356
株式会社パンプキンハウス
神奈川県厚木市飯山1620番地の１　アメニテイヒル本厚木717

(72)発明者　佐々木　実
神奈川県厚木市飯山1620番地の１　アメニテイヒル本厚木717

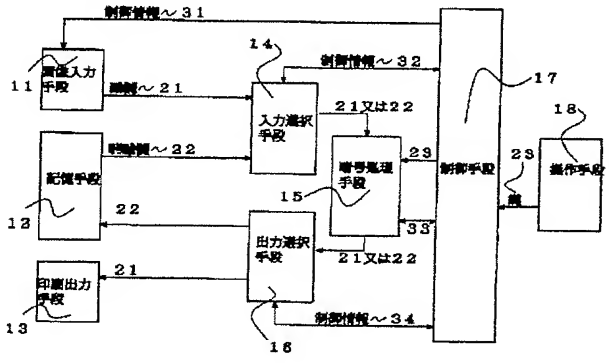
(72)発明者　吉川　博晴
神奈川県座間市緑が丘５丁目４番27号　グリーンヒルサノ１－121

(54)【発明の名称】　暗号機能付き複写機

(57)【要約】　(修正有)

【目的】　保管しようとする書類、図面の画像情報を暗号化した状態で記憶手段又は携帯可能な記憶手段に記憶し、必要に応じて記憶手段から暗号画像情報を正しく読みだして復号し、元の画像情報を印刷及び／またはデイスプレイに表示可能な暗号機能付き複写機を実現する。

【構成】　画像入力手段と暗号処理手段と印刷出力手段及び／またはデイスプレイ手段とを具備した暗号機能付き複写機に、暗号画像情報の記憶を行う記憶手段又は携帯可能な記憶手段をさらに具備する。また、暗号画像情報を種々のノイズから防御するために、さらに同期用符号付加手段を具備及び／または圧縮符号符号化手段と圧縮符号復号手段とを具備及び／または誤り訂正符号化手段と誤り訂正復号手段とを具備する。また、暗号処理に用いる鍵の決定と管理を簡便にするため、鍵生成手段又は鍵共有方式暗号システム（ＫＰＳ）を用いた鍵生成手段をさらに具備する。



1

【特許請求の範囲】

【請求項１】　画像入力手段と暗号処理手段と記憶手段と印刷出力手段及び／またはデイスプレイ手段を具備し、紐などの媒体に描写された画像情報を前記画像入力手段で入力し、これを前記暗号処理手段で暗号化して前記記憶手段に記憶させ、また、前記記憶手段に記憶された暗号画像情報を読みだして前記暗号処理手段で復号し、元の画像に戻して印刷及び／またはデイスプレイに表示を行うことを特徴とする暗号機能付き複写機。

【請求項２】　前記記憶手段が携帯可能であることを特徴とする請求項１の暗号機能付き複写機。

【請求項３】　同期用符号付加手段をさらに具備し、暗号化時に、前記同期用符号付加手段が、前記暗号画像情報に同期用符号を付加して前記記憶手段に記憶し、復号時に、前記同期用符号が付いた暗号画像情報から前記同期用符号を認識して同期を取りながら前記暗号画像情報の復号を行うことを特徴とする請求項１から請求項２の暗号機能付き複写機。

【請求項４】　圧縮符号化手段と圧縮符号復号手段をさらに具備し、入力した画像情報を前記圧縮符号化手段を用いて符号化して圧縮した後前記暗号処理手段で暗号化して暗号画像情報を作成し、又、前記暗号画像情報を前記暗号処理手段で復号して圧縮符号化画像情報とした後、前記圧縮符号復号手段で元の画像情報に戻すことを特徴とする請求項１から請求項３の暗号機能付き複写機。

【請求項５】　誤り訂正符号化手段と誤り訂正復号手段をさらに具備し、前記暗号画像情報に前記誤り訂正符号化手段で誤り訂正符号を生成して付加し、また、誤り訂正符号を含む前記暗号画像情報に対して、前記誤り訂正復号手段で復号を行った後、前記暗号処理手段で復号を行い元の画像情報に戻すことを特徴とする請求項１から請求項４の暗号機能付き複写機。

【請求項６】　鍵生成手段をさらに内蔵させたことを特徴とする、請求項１から請求項５の暗号機能付き複写機。

【請求項７】　前記鍵生成手段を内蔵した外部装置を接続し、外部装置内で生成させた暗号鍵を用いて暗号化／復号を行うことを特徴とする請求項１から請求項６の暗号機能付き複写機。

【請求項８】　前記鍵生成手段と暗号処理手段とを内蔵した外部装置を接続し、外部装置内で暗号鍵の生成と画像情報の暗号化または暗号画像の復号を行うことを特徴とする請求項１から請求項７の暗号機能付き複写機。

【請求項９】　各エンテイテイ（人、装置、名前等）が、半固定的に用いるもので任意に定められる公開の識別子を有し、センタ（管理者）だけが持つ特別なアルゴリズム（データ）と、エンテイテイの識別子に一方向性でランダムな単射を行う識別子変換を施したものとを演算させて、エンテイテイに固有な秘密アルゴリズム（データ）を生成してエンテイテイがこれを保持し、暗号化／復号を行う際に任意のエンテイテイの識別子または任意の名前等を識別子として識別子変換を施したものと自分の秘密アルゴリズムとを演算させることにより、打合せや第三者による配送を必要とせずに、自分と任意のエンテイテイ又は任意の名前等に固有の鍵（暗号鍵）を生成する鍵共有方式暗号システム（ＫＰＳ）による共有鍵生成手段を具備し、前記共有鍵生成手段で生成した鍵を用いて、前記画像情報の暗号化／復号を行うことを特徴とする請求項１から請求項８の暗号機能付き複写機。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は暗号機能付き複写機に関する。

【０００２】

【従来技術】書類、図面などの画像情報を複写機で複写を行うようにして入力し、暗号化した状態で印刷して保管することによって内容の漏洩を防ぎ、必要なときに復号して元に戻すことを可能とした暗号機能付き複写機が提案された。

【０００３】

【発明が解決しようとする問題点】保管しようとする書類、図面の画像情報を読取って暗号化し、暗号化した状態で印刷（暗号複写）することで書類、図面の内容は秘匿される。しかしながら、一般に印刷物を保管する場合、空間的にも重量的にも大きくなることや、紙質の経時変化に対する保全やバックアップ上の見地から、他の記憶媒体に記録することが求められている。また、記憶した暗号画像情報は、元の書類や図面のようにその所有者が個人で管理できなければならない。また、暗号画像情報は正しく記憶手段に記憶され、また記憶手段から正しく読み出されて復号され、元の画像情報に戻らなければならないと共に、種々のノイズに対して防御されている必要がある。また、暗号処理に必要な鍵の決定やその管理は簡易に行われなければならない。

【０００４】

【課題を解決する為の手段】上記問題に鑑み、本発明は、保管しようとする書類、図面の画像情報を暗号化した状態で記憶手段或いは携帯可能な記憶手段に記憶することにより、不正な読みだしから内容を保護することを可能とし、必要に応じて記憶手段に記憶された暗号画像情報を読み出して復号し、元の書類図面を印刷及び／またはデイスプレイに表示させることを可能とする暗号機能付き複写機を実現する。また、暗号化時に暗号情報に対する同期符号を暗号画像情報に付加して前記記憶手段に記憶し、復号時にこれを読取って暗号画像情報と同期を取りながら復号することで、記憶手段からの読みだしの精度を高める暗号機能付き複写機を実現する。又、入力した画像情報を符号化して圧縮した後暗号化することにより、記憶する暗号化情報を少くし、さらに、暗号化

時に暗号情報に対する誤り訂正符号を生成して暗号画像情報に付加して前記記憶手段に記憶し、復号時にこれを読取って暗号画像情報の誤り訂正を行って復号することで、記憶手段への書込み、読みだし、その他の処理にともなって発生した誤りに対して元の暗号画像情報を復元することが可能な暗号機能付き複写機を実現する。さらに、暗号化時に鍵を生成する鍵生成手段を備えることにより鍵設定を容易にすると共に、これに鍵共有方式暗号システム（ＫＰＳ）による鍵生成手段を用いて構成することにより、打合わせや第三者による鍵の配送を必要としない暗号機能付き複写機を実現する。また、前記鍵生成手段または前記鍵生成手段と暗号処理手段を外部装置に接続させる構成にすることにより、本発明による装置を使用する複数の人間が自分の書類、図面を個別に管理することを可能とする。

【０００５】

【実施例】図１は本発明の暗号機能付き複写機の一実施例を示した図である。本暗号機能付き複写機（以下、本機と称する）は、複写を行う書類、図面の画像入力手段（１１）、暗号化された画像情報を記憶する記憶手段（１２）、画像情報を用紙に印刷する印刷出力手段（１３）、画像入力手段（１１）と記憶手段（１２）から入力情報の選択を行う入力選択手段（１４）、入力した書類、図面の画像情報の暗号化または暗号画像情報の復号を行う暗号処理手段（１５）、暗号処理手段（１５）から出力された暗号または復号画像情報（２２）、（２１）を記憶手段（１２）または印刷出力手段（１３）に出力する出力選択手段（１６）、各手段の制御を行う制御手段（１７）及びユーザが本機を操作する為の操作手段（１８）から構成される。

【０００６】本機を用いて書類図面を暗号化し、記憶手段に記憶させる一例を説明する。書類図面は、制御情報（３２）の指示により入力選択手段（１４）で画像入力手段（１１）が選択されて画像情報（２１）として入力され、暗号処理手段（１５）へ送られて制御手段（１７）によって設定された暗号鍵（２３）を用いて暗号化される。暗号化された暗号化画像情報（２２）は、出力選択手段（１６）に送られた後、制御情報（３４）の指示で記憶手段（１２）に出力されて記憶される。

【０００７】次に、復号について説明する。記憶手段（１２）に記憶された書類、図面の暗号画像情報（２２）は、制御情報（３２）の指示で入力選択手段（１４）から入力データとして入力され、暗号処理手段（１５）へ送られて制御手段（１７）が設定した暗号鍵（２３）を用いて復号される。復号された画像情報（２１）は、出力選択手段（１６）で制御情報（３４）の指示により印刷出力手段（１３）に送られて用紙上に元の書類、図面の画像情報を印刷出力する。以上により、画像情報は暗号化されて本装置に具備された記憶手段に記憶され、必要に応じて読みだされて復号し、元の書類、図面の画像情報を用紙上に印刷出力される。

【０００８】次に、本発明請求項２の一実施例を図１、図２を用いて説明する。本発明請求項２は、図１における前記記憶手段（１２）を携帯可能としたもので、その実施例を図２に示す。図２で、記憶手段（１２）は、インタフェース手段（４１）によって入力選択手段（１４）と出力選択手段（１６）に接続され、分離して携帯可能となっている。記憶手段（１２）としては、フロッピーデイスクや光デイスクや差し替え可能なＲＯＭ、メモリ基板など取り外しが可能な記憶手段であれば何でも良い。インタフェース手段としては、フロッピーデイスクにおけるフロッピーデイスクドライバーなどがある。これにより、本機を使用する複数の人間が、自分の書類、図面等の情報を個別に管理することを可能としている。

【０００９】次に、本発明請求項３による一実施例を図３に示し、その詳細を図１、図３を用いて説明する。本発明請求項３は、図１の構成に対し同期用符号付加手段（４２）を更に具備したもので、その他は図１と同じである。暗号化時は、画像入力手段（１１）で読取った画像情報（２１）を暗号処理手段（１５）に送って暗号化する。暗号画像情報（２２）は、出力選択手段（１６）から同期用符号付加手段（４２）に送られ、同期用符号が付加された暗号画像情報（２５）として記憶手段（１２）に記憶される。復号時は、前記暗号画像情報（２５）が前記記憶手段（１２）から前記暗号処理手段（１５）に送られる。ここで、前記制御手段（１７）は、前記暗号画像情報（２５）の同期用符号にしたがって同期を取りながら前記暗号処理手段（１５）に復号させ、復号した画像情報（２１）を印刷出力手段（１３）に送って印刷出力させる。これにより、ノイズなどから画像情報の読取り誤りを防止することを可能としている。

【００１０】次に、本発明請求項４による一実施例を図４に示し、詳細を図１、図４を用いて説明する。本発明請求項４は、図１に対して圧縮符号化手段（４４）と圧縮符号復号手段（４５）を更に具備したもので、その他は図１と同じである。暗号化時は、入力された画像情報（２１）を、圧縮符号化手段（４４）で符号化して符号化画像情報（２６）とし、暗号処理手段（１５）に送り、暗号化して暗号画像情報（２２）として記憶手段（１２）へ送る。復号時は、前記記憶手段（１２）から前記暗号画像情報（２２）が読みだされ、暗号処理手段（１５）で復号されて符号化画像情報（２６）とし、圧縮符号復号手段（４５）で復号が行われて元の画像情報（２１）に戻り、印刷出力手段（１３）で印刷出力される。画像情報を圧縮し情報量を少くして暗号化を行うため、暗号化の時間を短縮すると共に、同じ容量の記憶手段に記憶可能な暗号画像情報量を大きくすることが出来る。更にまた、暗号画像情報の大きさが小さいため、記憶手段への書込みや読みだしの際に生ずる誤りの発生頻

度を少くすることが出来る。

【００１１】次に、本発明請求項５による一実施例を図５に示し、詳細を図１、図５を用いて説明する。本発明請求項５は、図１の構成に対し誤り訂正復号手段（４６）と誤り訂正符号化手段（４７）を更に具備したもので、その他は図１と同じである。暗号化時は、画像入力手段（１１）で読取った画像情報（２１）を暗号処理手段（１５）に送って暗号画像情報（２２）とし、誤り訂正符号化手段（４７）で誤り訂正符号を付加して符号化暗号画像情報（２７）とし、出力選択手段（１６）に送って記憶手段（１２）への記憶を行わせる。復号時は、前記記憶手段（１２）から前記符号化暗号画像情報（２７）が読みだされ、誤り訂正復号手段（４６）で誤り訂正が行われ、暗号画像情報（２２）として暗号処理手段（１５）に送られ、復号されて元の画像情報に戻り、印刷出力手段（１３）で印刷出力される。これにより、ノイズなどから暗号画像情報の読取り、書込みの誤りを防止すると共に、記憶手段における情報誤りを防止することを可能としている。

【００１２】次に、本発明請求項６による一実施例を図６に示し、詳細を図１、図６を用いて説明する。本発明請求項６は、図１の構成に対し鍵生成手段（５１）を更に具備したもので、その他は図１と同じである。実施例では、暗号化（復号）に用いる鍵（２３）を生成させる鍵生成指示情報（３５）を操作手段（１８）から鍵生成手段（５１）に入力し、鍵生成手段（５１）は、前記鍵生成指示情報（３５）に従って前記鍵（２３）を生成し、前記暗号処理手段（１５）で使用する鍵としている。具体的には、鍵生成手段として乱数生成回路等を使用することが出来る。

【００１３】次に、本発明請求項７による一実施例を図７に示し、詳細を図１、図６、図７により説明する。本実施例は、インタフェース手段（６１）をさらに具備し、図６の実施例に於ける鍵生成手段（５１）を内蔵した外部装置（６２）を前記インタフェース手段（６１）により接続して脱着可能としたものであり、その他の構成は図１の実施例と同じである。操作手段（１８）から入力された情報又は識別子（２４）は、制御手段（１７）によって前記インタフェース手段（６１）から前記外部装置（６２）の鍵生成手段（５１）に送られ、生成された鍵（２３）は、制御手段（１７）により暗号処理手段（１５）に入力されて画像情報の暗号化又は復号に用いられる。本発明により、複数のエンテイテイが独自に鍵生成手段を内蔵した外部装置を所有することによって、一台の本発明のよる暗号機能付き複写機をそれぞれのエンテイテイが独自に鍵を管理して使用することを可能とした。

【００１４】次に、本発明請求項８による一実施例を図８に示し、詳細を図７、図８を用いて説明する。本発明請求項８は、図７の実施例から暗号処理手段（１５）を除去し、図７の外部装置（６２）にさらに暗号処理手段（５２）を内蔵させたものである。その他の手段は図７と同じである。暗号化時は、暗号化に用いる前記鍵（２３）を特定する情報又は識別子（２４）が制御手段（１７）によりインタフェース手段（６１）を通って前記外部装置（６１）の鍵生成手段（５１）に入力され、鍵（２３）が生成される。又、画像入力手段（１１）から読みだされ、入力選択手段（１４）で入力された画像情報（２１）が前記外部装置（６２）の暗号処理手段（１５）に送られ、生成された前記鍵（２３）を用いて暗号化されて暗号画像情報（２２）となり、再び前記インタフェース手段（６１）を通って出力選択手段（１６）に送られ、記憶手段（１２）に記憶される。復号時は、前記記憶手段（１２）から読みだされた暗号画像読取り手段（２２）が、暗号化と同様にして前記外部装置（６２）の暗号処理手段（５２）に送られ、前記鍵生成手段（５１）で生成した鍵（２３）を用いて復号されて画像情報（２１）となり、出力選択手段（１６）に送られ、印刷出力手段（１３）で印刷出力される。本発明請求項８は、暗号化とそれに用いる鍵の生成を外部装置内で行うため、複数のエンテイテイが独自に鍵生成手段と暗号処理手段とを内蔵した外部装置を所有して、一台の本発明による暗号機能付き複写機をそれぞれのエンテイテイが独自で鍵を管理して使用することを可能とした。

【００１５】次に、本発明請求項９による鍵生成手段の一実施例を図９に示し、詳細を図６、図９を用いて説明する。本発明請求項９の実施例の説明は、図６における鍵生成手段（５１）を、図９の鍵共有方式暗号システム（ＫＰＳ）による共有鍵生成手段の実施例に替えて構成したものとして行う。図９の実施例は、識別子変換手段（５２）と秘密アルゴリズム格納手段（５３）と共有鍵生成手段（５４）で構成される。図６の操作手段（１８）から入力されたエンテイテイ（人、装置、名前等）の識別子（２４）は、制御手段（１７）により図９の識別子変換手段（５２）に送られ、識別子変換手段（５２）で変換された識別子（２８）は、共有鍵生成手段（５４）に送られる。共有鍵生成手段（５４）では、変換された前記識別子（２８）と、秘密アルゴリズム格納手段（５３）に格納された秘密アルゴリズム（２９）とを演算させて自分とエンテイテイとの固有な共有鍵を生成させ、これを鍵（２３）として図６の暗号処理手段（１５）に送って暗号化または復号に用いられる。

【００１６】ここで、打合せや第三者による暗号鍵（鍵）の配送を必要とせずに、自分と任意のエンテイテイに固有の鍵を生成する鍵共有方式暗号システム（ＫＰＳ）について説明する。エンテイテイとは、一般に通信に於ける当事者となる人や装置などを示すが、ここでは人間、文書図面、装置、及びそれらを構成要素とするシステムを含む。

【００１７】エンテイテイｉが、半固定的に用いるもの

で任意に定められる公開の識別子を有し、これを識別子Ｙｉとし、これに一方向性でランダムな単射を行う識別子変換Ｆを施したものをＺｉ（数式１）とする。センタだけが持つ特別なアルゴリズム（データ）Ｇと、前記Ｚｉとを演算させて、エンテイテイｉに固有な秘密アルゴリズム（データ）Ｘｉ（数式２）を生成する。

【数１】Ｚｉ＝Ｆ（Ｙｉ）

【数２】Ｘｉ＝Ｇ（Ｚｉ）

エンテイテイｉは、自分の秘密アルゴリズムＸｉにエンテイテイｊの識別子Ｙｊを識別子変換したものＺｊまたは任意の名前等を識別子Ｙｘとして識別子変換したものＺｘを入力し、演算させて（数式３、４）、エンテイテイｊとの共通な暗号鍵ｋｉｊまたは任意の名前に固有の暗号鍵ｋｉｘを生成させることができる。またエンテイテイｊの秘密アルゴリズムＸｊに、エンテイテイｉの識別子Ｙｉを識別子変換したＺｉを入力して演算し（数式５）、鍵ｋｊｉを生成させることができ、これが前記ｋｉｊに等しい（数式６）ので、エンテイテイｉが暗号鍵ｋｉｊで暗号化した内容は、エンテイテイｊに復号させることができる。暗号鍵ｋｉｘを用いて暗号化した内容は、秘密アルゴリズムＸｉを持つエンテイテイｉ以外では復号できない。

【数３】ｋｉｊ＝Ｘｉ（Ｚｊ）

【数４】ｋｊｉ＝Ｘｊ（Ｚｉ）

【数５】ｋｉｊ＝ｋｊｉ＝ｋ

【数６】ＫＰＳの理論的な詳細ついては、文献１から文献５等に記述されている。

【００１８】

【発明の効果】本発明は、書類、図面等の画像情報を暗号化して記憶手段に記憶させ、必要な時に再び書類、図面等の状態に戻すことを可能にした。これは、大切な情報を秘密裏に、しかも、記憶手段を携帯可能とすることで、複数の人間が本発明の装置を使用し、暗号化して記憶された情報を各々が自分で保管することを可能とした。また、同期用符号付加手段を具備することにより画像情報の暗号化と復号に於ける再現性を向上させ、圧縮符号による符号化（復号）手段を具備することにより必要な記憶容量を小さくし、さらに、誤り訂正符号化（復号）手段を具備することにより、信頼性を向上させた。又、鍵生成手段を内蔵させたことにより、暗号化時の鍵設定を容易にすると共に、鍵生成手段および暗号処理手段を脱着可能な外部装置とすることによって、本発明による装置を使用する複数の人間がそれぞれ独時に鍵を管理して使用することを可能とした。さらに、鍵共有方式暗号システム（ＫＰＳ）による共有鍵生成手段を用いて暗号化（復号）の鍵を生成させて使用することにより、鍵の設定と管理を一段と向上させた暗号機能付き複写機を実現した。

【図面の簡単な説明】

【図１】本発明請求項１の一実施例とその動作を示す図である。

【図２】本発明請求項２の一実施例とその動作を示す図である。

【図３】本発明請求項３の一実施例とその動作を示す図である。

【図４】本発明請求項４の一実施例とその動作を示す図である。

【図５】本発明請求項５の一実施例とその動作を示す図である。

【図６】本発明請求項６の一実施例とその動作を示す図である。

【図７】本発明請求項７の一実施例とその動作を示す図である。

【図８】本発明請求項８の一実施例とその動作を示す図である。

【図９】本発明請求項９の鍵生成手段の一実施例とその動作を示す図である。

【符号の説明】

１１	画像入力手段
１２	記憶手段
１３	印刷出力手段
１４	入力選択手段
１５	暗号処理手段
１６	出力選択手段
１７	制御手段
１８	操作手段
２１	画像情報
２２	暗号画像情報
２３	暗号鍵（鍵）
２４	情報又は識別子
２５	同期用符号を付加した暗号画像情報
２６	符号化画像情報
２７	符号化暗号画像情報
２８	変換された識別子
２９	秘密アルゴリズム
３１	制御手段～画像入力手段間の制御情報
３２	制御手段～入力選択手段間の制御情報
３３	制御手段～暗号処理手段間の制御情報
３４	制御手段～出力選択手段間の制御情報
３５	鍵生成指示情報
４１	インタフェース手段
４２	同期用符号付加手段
４４	圧縮符号化手段
４５	圧縮符号復号手段
４６	誤り訂正復号手段
４７	誤り訂正符号化手段
５１	鍵生成手段
５２	識別子変換手段
５３	秘密アルゴリズム格納手段
５４	共有鍵生成手段

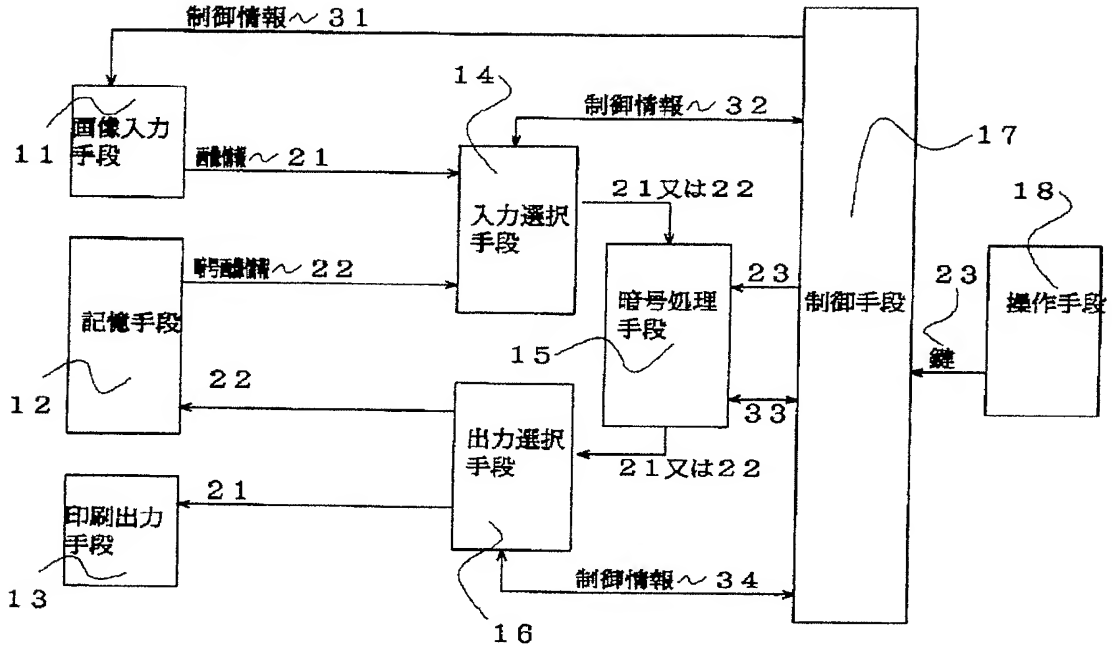
9

61　　インタフエース手段
62　　外部装置

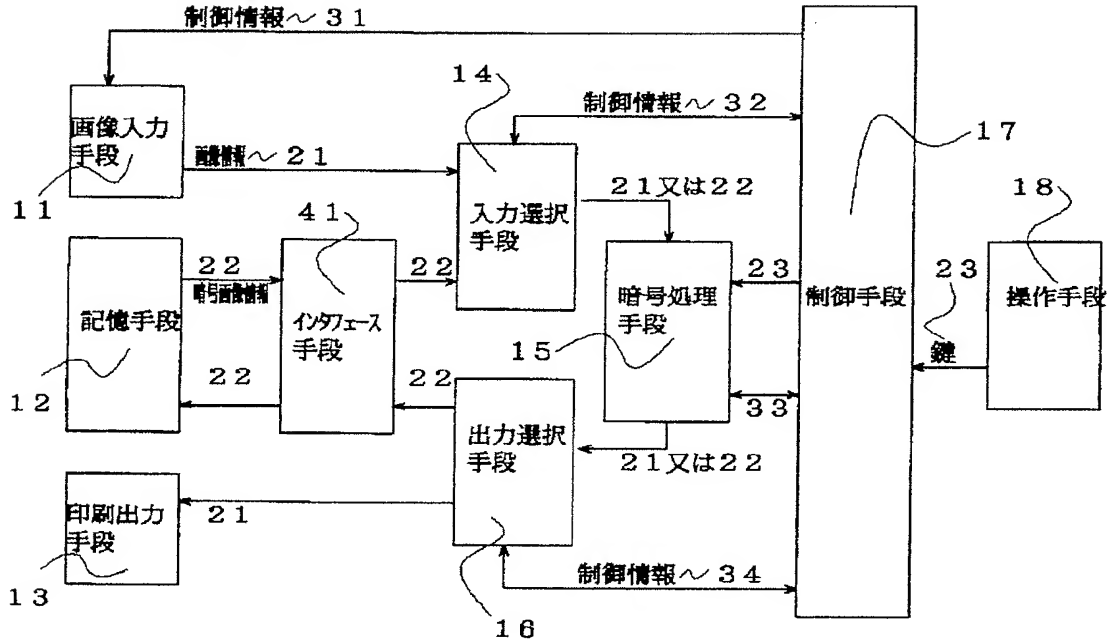
【文献1】松本勉、今井秀樹、”第3の鍵共有方式”、1986年暗号と情報セキュリテイワークショップ講演論文集、1986年8月。
【文献2】松本勉、今井秀樹、”簡便な暗号鍵共有方式”、電気通信学会誌IT86－54、P－29～34、1986年9月。
【文献3】松本勉、今井秀樹、”キー　プレデイストリビューション　システムの一方式”（”KEY PRE DISTRIBUSION SYSTEM BASED ON LINEAR ALGEBRA”）、第9回情報理論とその応用シンポジウム、SITA，86，1986年10月。
【文献4】松本勉、今井秀樹、”アプライング　ザ　キー　プレデイストリビューション　システム　トウ　エレクトリニク　メイル　アンド　シグネチュア”，情報理論とその応用シンポジウム、SITA’87，198＊7年11月。（Tsutomu MATSUMOTO and，Hideki IMAI，”Applying the Predistribution Systemto Electronic Mails and Signatures”，SITA’87，NOV.，1987.）
【文献5】松本勉、今井秀樹、”パフォーマンス　オブ　リニア　スキーム　フォア　ザ　キー　プレデイストリビューション　システム”、IEICE情報セキュリテイ技術報告、5月20日号、1989年。（Tsutomu MATSUMOTO and，Hideki IMAI，”Performance of linear schemes for the Key Predistribution System”，IEICETechnical report on Information Security，May 20，1988.）

10

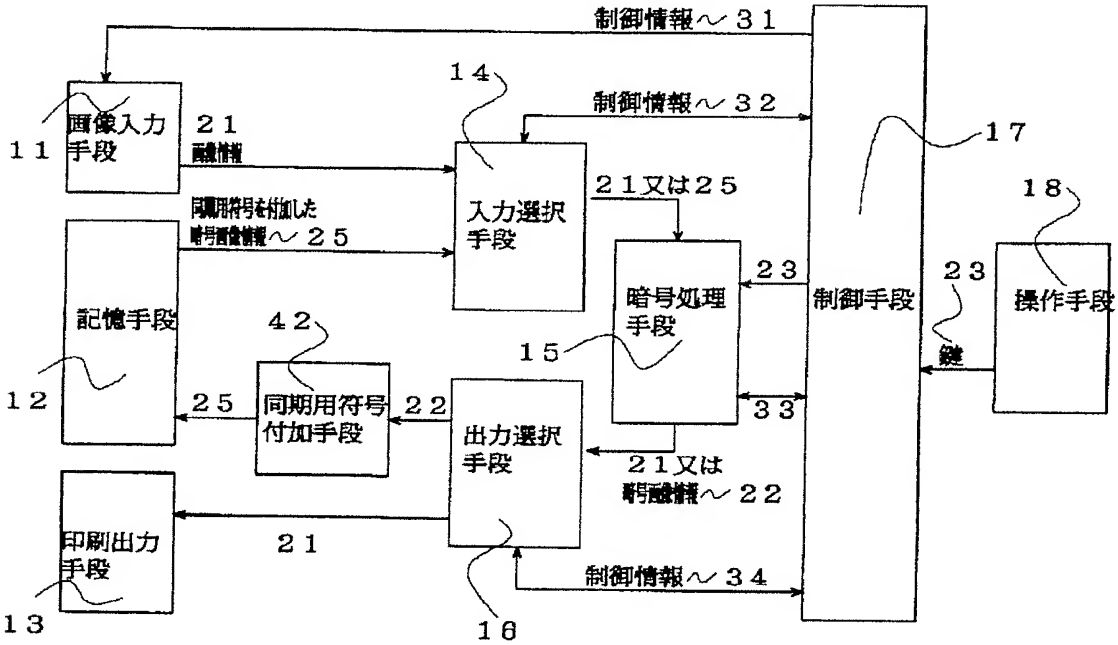
【図1】



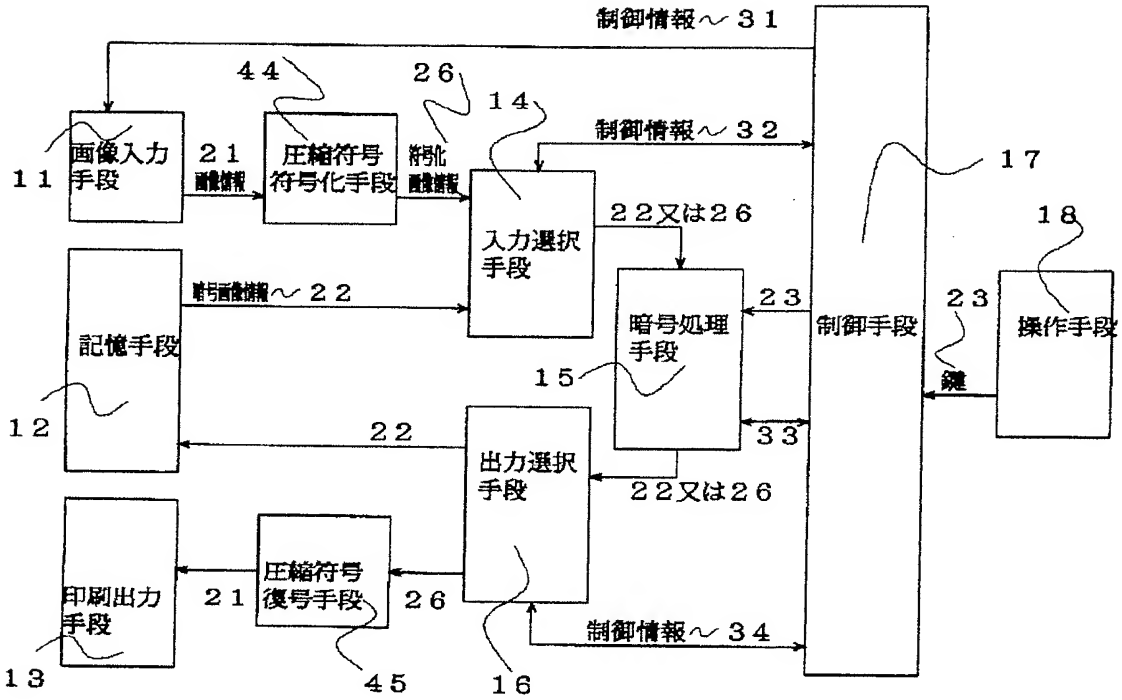
【図２】


制御情報～３１
１４
制御情報～３２
１７
画像入力手段
画像情報～２１
２１又は２２
１８
１１
４１
入力選択手段
２２
２２
２３
２３
記憶手段
暗号画像情報
インタフェース手段
暗号処理手段
制御手段
操作手段
１５
鍵
２２
２２
３３
１２
出力選択手段
２１又は２２
印刷出力手段
２１
制御情報～３４
１３
１６

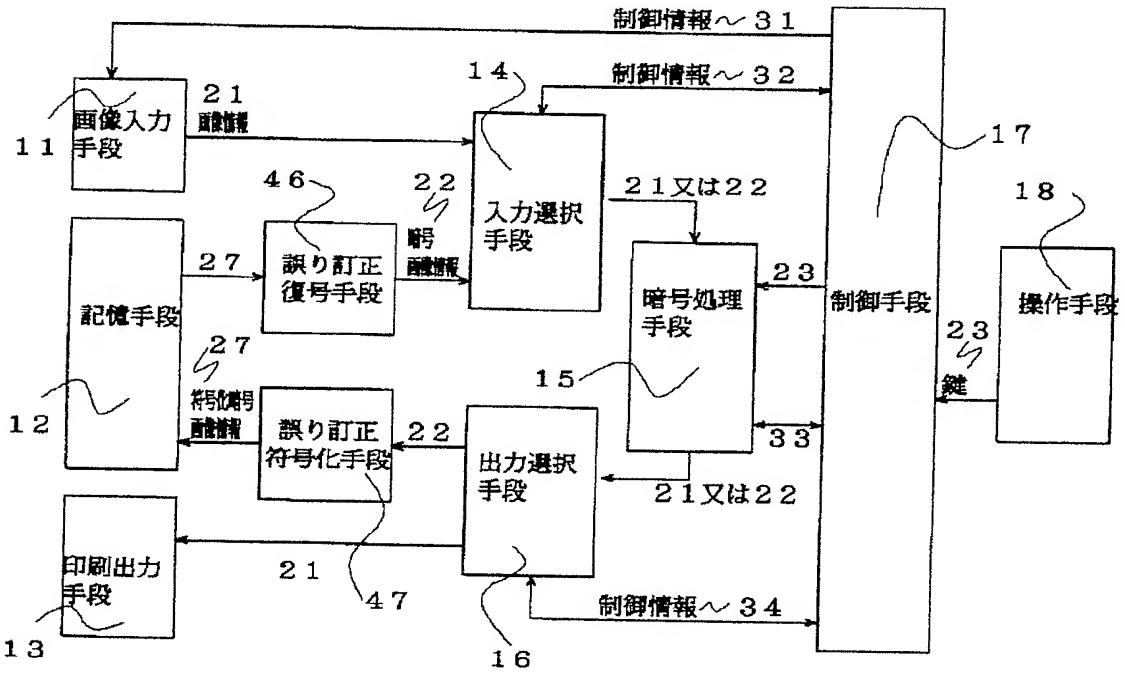
【図３】


制御情報～３１
１４
制御情報～３２
１７
画像入力手段
２１
画像情報
２１又は２５
１８
１１
同期用符号を付加した暗号画像情報～２５
入力選択手段
２３
２３
記憶手段
暗号処理手段
制御手段
操作手段
４２
１５
鍵
１２
２５
同期用符号付加手段
２２
出力選択手段
３３
２１又は暗号画像情報～２２
印刷出力手段
２１
制御情報～３４
１３
１６

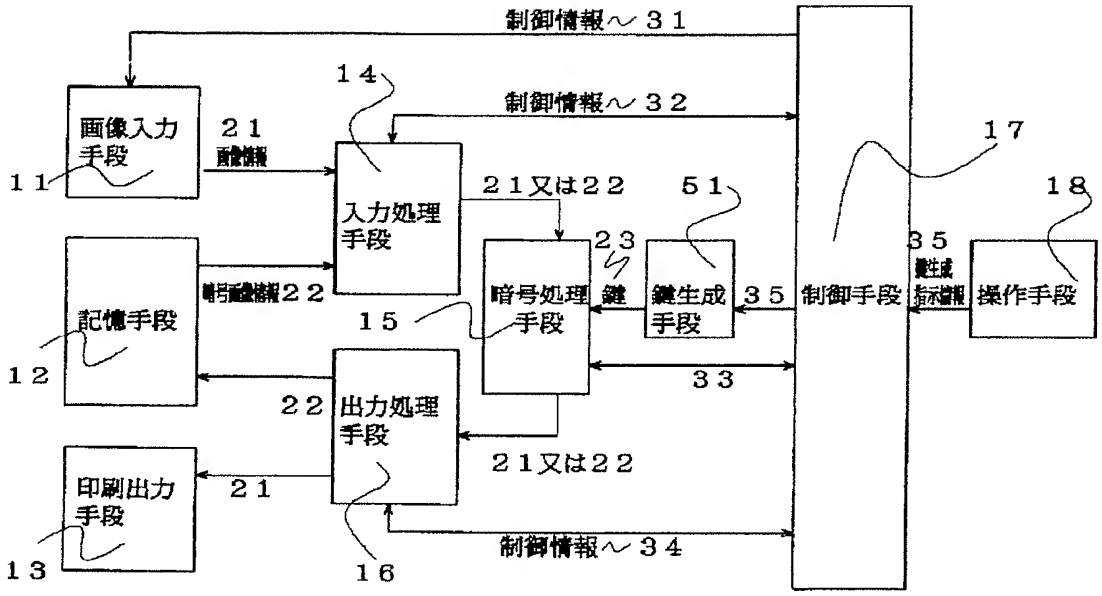
【図４】


制御情報～３１
４４
２６
１４
１１
画像入力手段
２１
圧縮符号化手段
制御情報～３２
１７
２２又は２６
１８
入力選択手段
暗号画像情報～２２
２３
２３
記憶手段
暗号処理手段
制御手段
操作手段
１５
鍵
１２
２２
３３
出力選択手段
２２又は２６
印刷出力手段
圧縮符号復号手段
２１
２６
制御情報～３４
１３
４５
１６

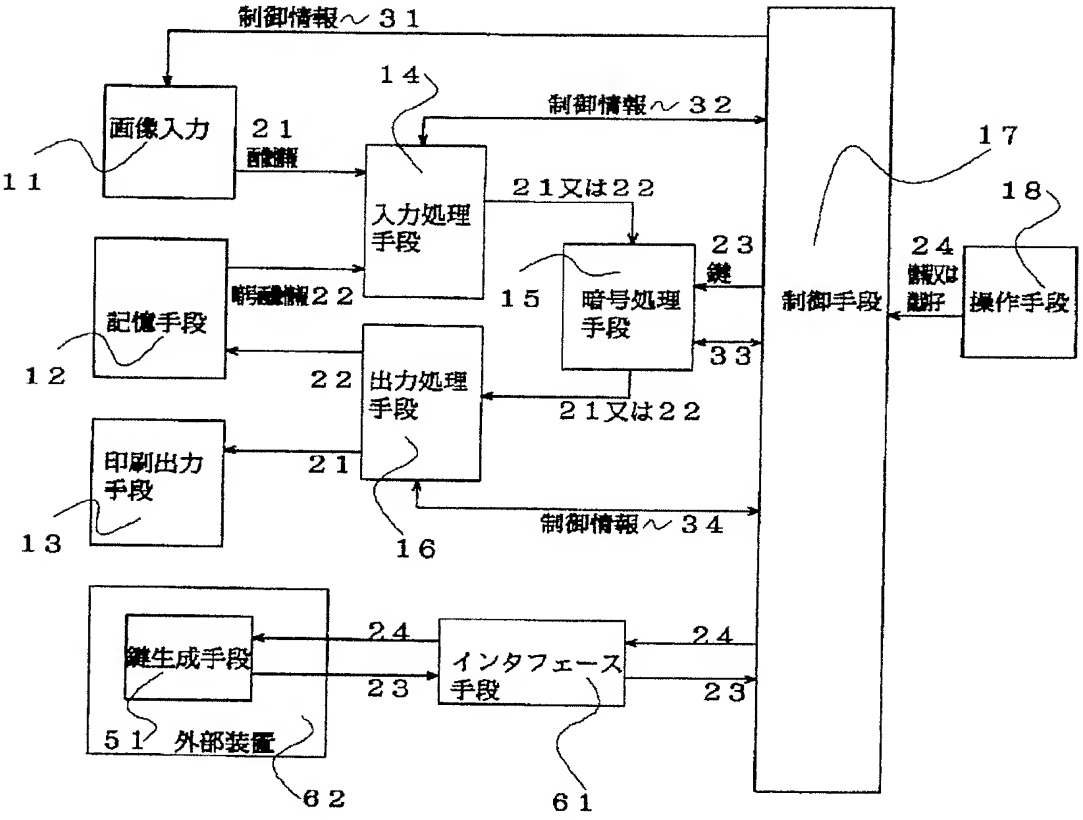
【図５】


制御情報～３１
１４
制御情報～３２
２１
１１
画像入力手段
１７
４６
２２
２１又は２２
１８
入力選択手段
２７
誤り訂正復号手段
暗号画像情報
２３
暗号処理手段
制御手段
操作手段
記憶手段
２７
２３
１５
鍵
符号化暗号画像情報
誤り訂正符号化手段
２２
出力選択手段
１２
３３
２１又は２２
印刷出力手段
２１
４７
制御情報～３４
１３
１６

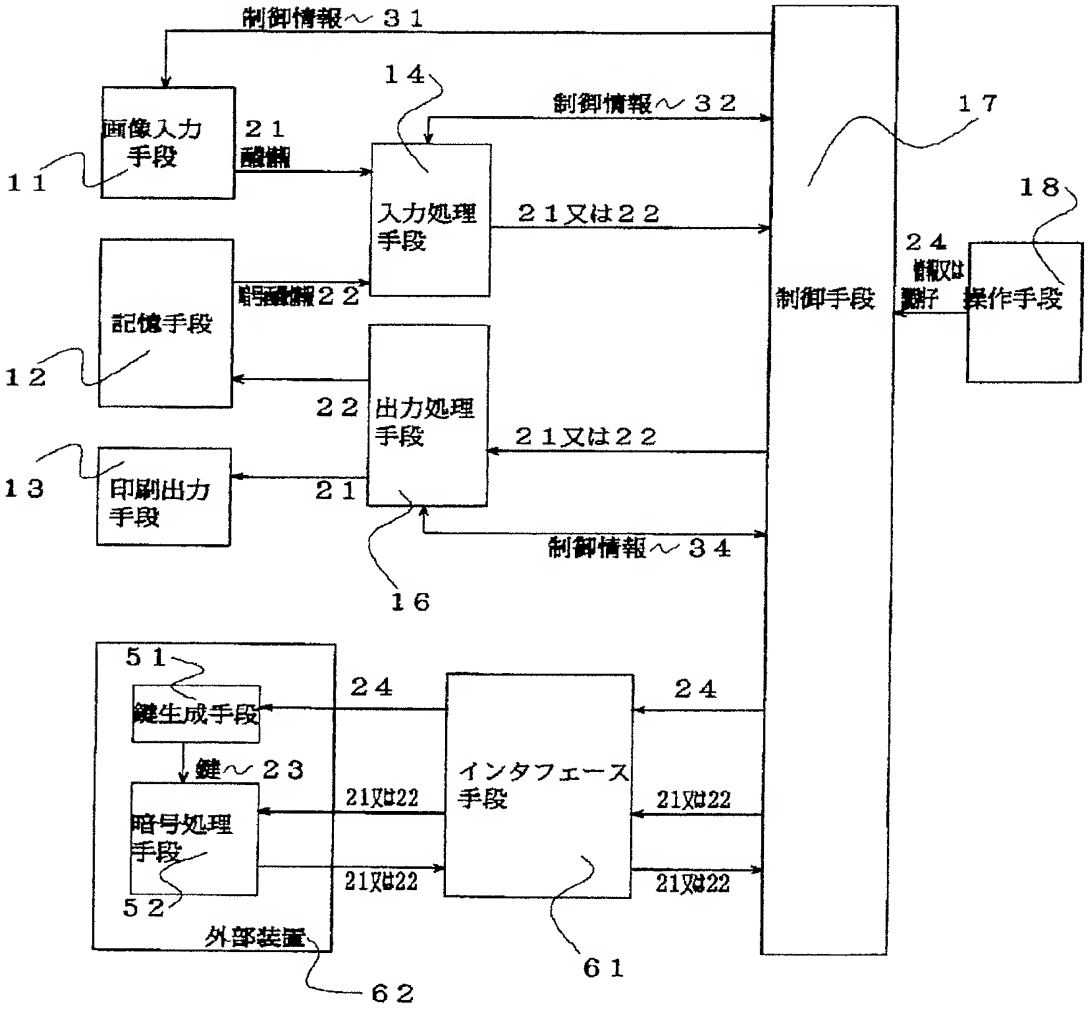
【図６】


制御情報～３１
１４
制御情報～３２
１７
画像入力手段
２１
画像情報
１１
入力処理手段
２１又は２２
５１
１８
２３
３５
暗号化鍵情報２２
暗号処理手段
鍵
鍵生成手段
３５
制御手段
鍵生成指示情報
操作手段
１５
記憶手段
１２
３３
２２
出力処理手段
２１又は２２
印刷出力手段
２１
制御情報～３４
１３
１６

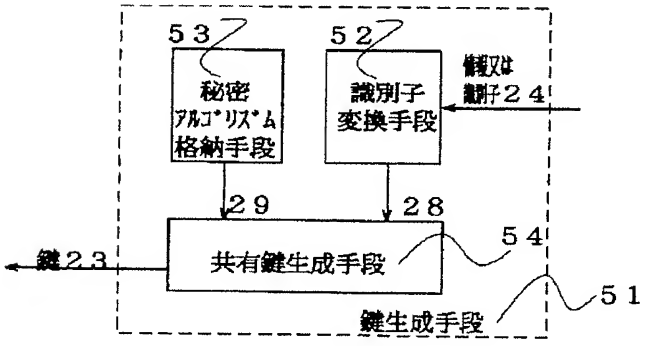
【図７】


制御情報～３１
１４
制御情報～３２
１７
画像入力
２１
画像情報
１１
入力処理手段
２１又は２２
１８
２３
鍵
２４
情報又は鍵好
暗号化鍵情報２２
１５
暗号処理手段
記憶手段
制御手段
操作手段
１２
３３
２２
出力処理手段
２１又は２２
印刷出力手段
２１
制御情報～３４
１３
１６
２４
２４
鍵生成手段
インタフェース手段
２３
２３
５１
外部装置
６２
６１

【図８】


制御情報～３１
１４
制御情報～３２
１７
画像入力手段
２１
１１
入力処理手段
２１又は２２
１８
２４
制御手段
操作手段
記憶手段
１２
２２
出力処理手段
２１又は２２
１３
印刷出力手段
２１
制御情報～３４
１６
５１
２４
２４
鍵生成手段
鍵～２３
インタフェース手段
暗号処理手段
５２
外部装置
６２
６１

【図９】


５３
５２
秘密ｱﾙｺﾞﾘｽﾞﾑ格納手段
識別子変換手段
２９
２８
５４
鍵２３
共有鍵生成手段
５１
鍵生成手段